LISTING OF THE CLAIMS:

1-21. (Canceled)

22. (Currently Amended) A method for populating password data to a target datastore [[of]]associated with a target user authenticator that is in communication with a source user authenticator after migration from [[a]]the source user authenticator, the source user authenticator ~~having~~ associated with a source datastore comprising unencrypted user identification data and user authentication data encrypted with a proprietary encryption algorithm, while also responding to user requests for information, the method comprising:

migrating unencrypted data from the source datastore to the target datastore~~, wherein the source datastore comprises user identification data and user authentication data, wherein the source datastore is associated with a source user authenticator, wherein the target datastore is associated with a target user authenticator, and wherein the target user authenticator is in communication with the source user authenticator~~;

intercepting, ~~with an~~ by a servlet interceptor, a request from a user to access information protected by the target user authenticator; ~~a request to the source user authenticator from a user seeking access to information protected by the target user authenticator, wherein the interceptor prompts~~

prompting, by the servlet interceptor, the user for an identification[[,]];

~~receives~~ receiving, by the servlet interceptor, the identification from the user[[,]];

locating, by the servlet interceptor, ~~locates~~ a corresponding identification in the target datastore[[,]]; [[and]]

~~searches~~ searching, by the servlet interceptor, the target datastore for a user authentication data associated with the corresponding identification;

determining, by the servlet interceptor, that the target datastore does not include a user authentication data associated with the corresponding identification;

forwarding the ~~original~~ intercepted request to the source user authenticator responsive to the determining ~~upon determining that the target datastore does not include a user authentication data associated with the corresponding identification~~;

~~using the source user authenticator to prompt~~ prompting, by the source user authenticator, the user for ~~and receive the~~ identification and user authentication data;

receiving, by the source user authenticator, identification and user authentication data from the user;

~~from the user,~~ monitoring, by a password capture process, ~~the target user authenticator: monitors~~ the source user authenticator for an approval response[[,]];

detecting, by the password capture process, ~~and upon an~~ the approval response from the source user authenticator[[,]];

~~captures~~ capturing, by the password capture process, the user authentication data provided to the source user authenticator by the user[[,]];

~~populates~~ populating, by the password capture process, the target datastore with the captured user authentication data associated with the corresponding identification upon detecting the approval response~~, and~~

~~associates the captured user authentication data with the corresponding identification~~.

23. (Previously Presented) The method of claim 22, wherein after populating the target datastore, further comprising prompting for and receiving from the user the user authentication data associated with the identification.

24. (Previously Presented) The method of claim 23, wherein the action of prompting for and receiving from the user the user authentication data associated with the identification comprises prompting for and receiving from the user the identification and the user authentication data associated with the identification.

25. (Currently Amended) The method of claim 22, wherein migrating unencrypted data from the source datastore to the target datastore comprises:

reading unencrypted data from the source datastore, ~~wherein the source datastore contains encrypted user authentication data and other unencrypted data,~~ wherein the unencrypted data represents data for multiple users each having an associated user identification and an associated user authentication data;

converting the unencrypted data to be compatible with the target datastore; and

populating the target datastore with the converted data.

26. (Previously Presented) The method of claim 22 further comprising:

authenticating the received identification using the target user authenticator upon determining that the target datastore includes user authentication data associated with the corresponding identification.

27. (Currently Amended) The method of claim 26, wherein authenticating the received identification further comprises prompting for and receiving from the user the user authentication data associated with the corresponding identification.

28. (Previously Presented) The method of claim 22, wherein the target datastore is an LDAP compliant directory service.

29. (Previously Presented) The method of claim 22, wherein the target datastore is a relational database.

30. (Previously Presented) The method of claim 22, wherein the source datastore is a relational database.

31. (Previously Presented) The method of claim 22, wherein the user is a person.

32. (Previously Presented) The method of claim 22, wherein the user is a software object.

33. (Previously Presented) The method of claim 22, wherein the user authentication data is a password.

34. (Previously Presented) The method of claim 22, wherein receiving user authentication form a user further comprises:

prompting for and receiving the identification and the user authentication data from the user after the initial submission of the identification from the user.

35. (Canceled)